



PTO/SB/21 (08-03)

Approved for use through 08/30/2003. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TRANSMITTAL
FORM**

(to be used for all correspondence after initial filing)

TRANSMITTAL FORM (to be used for all correspondence after initial filing)	Application Number	10/712,869	
	Filing Date	11/12/03	
	First Named Inventor	Keiichi Iwamura	
	Art Unit	2131	
	Examiner Name		
Total Number of Pages in This Submission	74	Attorney Docket Number	CFA00018US

ENCLOSURES (Check all that apply)

<input type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached <input type="checkbox"/> Amendment/Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input checked="" type="checkbox"/> Certified Copy of Priority Document(s) <input type="checkbox"/> Response to Missing Parts/ Incomplete Application <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s) _____	<input type="checkbox"/> After Allowance communication to Technology Center (TC) <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input type="checkbox"/> Other Enclosure(s) (please Identify below):
Remarks 		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Canon U.S.A., Inc. IP Department Fidel Nwamu
Signature	
Date	3/1/04

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Fidel Nwamu		
Signature		Date	3/1/04

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 0 月 3 日
Date of Application:

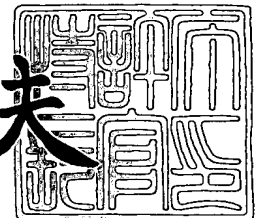
出 願 番 号 特 願 2 0 0 3 - 3 4 6 1 4 0
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 4 6 1 4 0]

出 願 人 キヤノン株式会社
Applicant(s):

2 0 0 3 年 1 2 月 2 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 256811
【提出日】 平成15年10月 3日
【あて先】 特許庁長官殿
【国際特許分類】 H04N 5/00
【発明者】
 【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社内
 【氏名】 岩村 恵市
【特許出願人】
 【識別番号】 000001007
 【氏名又は名称】 キヤノン株式会社
【代理人】
 【識別番号】 100090273
 【弁理士】
 【氏名又は名称】 國分 孝悦
 【電話番号】 03-3590-8901
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-332577
 【出願日】 平成14年11月15日
【手数料の表示】
 【予納台帳番号】 035493
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9705348

【書類名】 特許請求の範囲**【請求項 1】**

所定の作者により作成された原データを処理する情報処理装置であって、
前記原データを変更する際に、その変更に関する変更情報を保持する保持手段と、
前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする情報処理装置。

【請求項 2】

前記変更情報を正当なものとするかを判定する判定手段をさらに有し、
前記判定手段で正当なものとする判定された場合に、前記変更保証情報作成手段は、
前記変更保証情報を作成することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記原データが原本であることを保証するための原データ保証情報を保持する原データ保証情報保持手段をさらに有することを特徴とする請求項 1 または 2 に記載の情報処理装置。

【請求項 4】

前記原データを変更処理する変更処理手段をさらに有することを特徴とする請求項 1 ～ 3 の何れか 1 項に記載の情報処理装置。

【請求項 5】

前記変更保証情報と、前記原データ保証情報は、デジタル署名であることを特徴とする請求項 3 または 4 に記載の情報処理装置。

【請求項 6】

前記変更情報は、前記原データを特定する情報と、前記変更処理手段を特定する情報と、
前記原データを変更する際に行った変更処理を特定する情報とを含むことを特徴とする請求項 4 または 5 に記載の情報処理装置。

【請求項 7】

前記変更情報は、前記原データと、前記原データに対する変更データとの差分情報を含むことを特徴とする請求項 1 ～ 5 の何れか 1 項に記載の情報処理装置。

【請求項 8】

前記判定手段は、設定されたアクセス権限を用いて判定することを特徴とする請求項 2 ～ 7 の何れか 1 項に記載の情報処理装置。

【請求項 9】

前記判定手段は、前記原データの作者の公開鍵を用いて判定することを特徴とする請求項 2 ～ 7 の何れか 1 項に記載の情報処理装置。

【請求項 10】

前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを管理する管理手段をさらに有することを特徴とする請求項 3 ～ 9 の何れか 1 項に記載の情報処理装置。

【請求項 11】

前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを送付する送付手段をさらに有することを特徴とする請求項 3 ～ 9 の何れか 1 項に記載の情報処理装置。

【請求項 12】

所定の作者により作成された原データを処理する情報処理装置であって、
前記原データが原本として保証されたものであることを確認する原データ確認手段と、
前記原データの変更に関する変更情報が原本として保証されたものであることを確認する変更情報確認手段と、
前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、前記変更情報に応じて前記原データを変更する変更手段とを有することを特徴とする情報処理装置。

【請求項 13】

前記原データ確認手段は、前記原データに対するデジタル署名を検証し、前記変更情報確認手段は、前記変更情報に対するデジタル署名を検証するようにしたことを特徴とする請求項 12 に記載の情報処理装置。

【請求項 14】

前記請求項 3～9 の何れか 1 項に記載の情報処理装置とネットワークで接続されたサーバ装置であって、

前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを、前記情報処理装置より受信し、管理することを特徴とするサーバ装置。

【請求項 15】

ネットワークに接続された情報処理装置を複数有する電子データ管理システムであって、

前記情報処理装置は、前記ネットワーク上で共有された電子データが原本として保証されたものであることと、前記電子データの変更に関する第 1 の変更情報が原本として保証されたものであることを確認する確認手段と、

前記電子データと前記第 1 の変更情報が、前記確認手段により原本として保証されたものであることが確認された場合に、前記電子データを変更する電子データ変更手段と、

前記電子データ変更手段により変更された電子データの変更に関する第 2 の変更情報と、前記第 2 の変更情報が原本であることを保証するための変更保証情報とを作成する情報作成手段と、

前記情報作成手段により作成された第 2 の変更情報と、変更保証情報とを前記ネットワークに送信する送信手段とを有し、

前記複数の情報処理装置で共同して前記電子データの管理を行うようにしたことを特徴とする電子データ管理システム。

【請求項 16】

第 1 の情報処理装置と、前記第 1 の情報処理装置とネットワークを介して接続された第 2 の情報処理装置とを有する情報処理システムであって、

前記第 1 の情報処理装置は、前記第 1 の情報処理装置から電子データを受信する手段と

前記受信した電子データを変更し、その変更に関する変更情報と、前記変更情報が原本であることを保証するための第 1 の変更保証情報とを作成する手段と、

前記変更情報と前記第 1 の変更保証情報を、前記第 2 の情報処理装置に送信する手段とを有し、

前記第 2 の情報処理装置は、前記第 1 の情報処理装置により送信された変更情報が原本として保証されたものであることを、前記第 1 の変更保証情報を用いて確認する手段と、

前記変更情報を正当なものとするかを判定する手段と、

前記判定手段で正当なものとなると判定された場合に、前記変更情報が原本であることを保証するための第 2 の変更保証情報を作成する手段と、

前記第 2 の変更保証情報を、前記第 1 の情報処理装置に送信する手段とを有することを特徴とする情報処理システム。

【請求項 17】

所定の作者により作成された原データを処理する情報処理方法であって、

前記原データを変更する際に、その変更に関する変更情報を保持する保持工程と、

前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成工程とを行うことを特徴とする情報処理方法。

【請求項 18】

前記変更情報を正当なものとするかを判定する判定工程をさらに有し、

前記判定工程で正当なものとなると判定された場合に、前記変更保証情報作成工程は、前記変更保証情報を作成することを特徴とする請求項 17 に記載の情報処理方法。

【請求項 19】

所定の作者により作成された原データを処理する情報処理方法であって、

前記原データが原本として保証されたものであることを確認する原データ確認工程と、
前記原データの変更に係る変更情報が原本として保証されたものであることを確認する
変更情報確認工程と、

前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、
前記変更情報に応じて前記原データを変更する変更工程とを行うことを特徴とする情報
処理方法。

【請求項 2 0】

前記原データ確認工程は、前記原データに対するデジタル署名を検証し、前記変更情報
確認処理は、前記変更情報に対するデジタル署名を検証するようにしたことを特徴とする
請求項 1 9 に記載の情報処理方法。

【請求項 2 1】

前記請求項 1 7 ～ 2 0 の何れか 1 項に記載の情報処理方法をコンピュータに実行させる
ことを特徴とするコンピュータプログラム。

【請求項 2 2】

前記請求項 2 1 に記載のコンピュータプログラムを記憶することを特徴とするコンピュ
ータ読み取り可能な記憶媒体。

【書類名】明細書

【発明の名称】情報処理装置、サーバ装置、電子データ管理システム、情報処理システム、情報処理方法、コンピュータプログラム及びコンピュータ読み取り可能な記憶媒体

【技術分野】

【0001】

本発明は、情報処理装置、サーバ装置、電子データ管理システム、情報処理システム、情報処理方法、コンピュータプログラム及びコンピュータ読み取り可能な記憶媒体に関し、特に、データの原本性を保証するために用いて好適なものである。

【背景技術】

【0002】

近年、コンピュータやインターネットの普及に伴い、情報をデジタル化し、デジタルデータとして利用する形態が一般化しつつある。一方、デジタルデータでは、まったく同質なコピーを容易に生成でき、編集処理も容易に実行できるという特徴がある。そのため、デジタルデータの原本性を保証することは重要である。

【0003】

一般に、デジタルデータの原本性を保証するには、例えば、米国特許第5499294号明細書（特許文献1）に示されているように、デジタル画像のハッシュ値に公開鍵暗号を用いた電子署名を作成することによって実現できることが知られている。米国特許第5499294号明細書では、電子署名データを生成するために、ハッシュ関数と公開鍵暗号とを使用している。上記電子署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することができるようにするものである。

【0004】

ハッシュ関数と公開鍵暗号とを用いて電子署名データを生成してデータの正当性を確認する方法は、具体的に以下のようなものである。ここでは、米国特許第5499294号明細書に記載されている方法に、公知技術として知られている技術を付け加えて、わかりやすく説明する。

まず、秘密鍵を K_s 、公開鍵を K_p とすると、送信者は、平文データ M をハッシュ関数により圧縮して一定長の出力 h を算出する演算を行う（一定長の出力 h は、ハッシュ値と呼ばれる。）。

次に、秘密鍵 K_s で一定長の出力 h を変換して電子署名データ s を作成する演算を行う。この演算を以下の（1式）のように表現する。

$$D(K_s, h) = s \cdots (1 \text{ 式})$$

その後、該電子署名データ s と平文データ M とを受信者に送信する。

【0005】

一方、受信者は、受信した電子署名データ s を公開鍵 K_p で変換する演算を行う。この演算を以下の（2式）のように表現する。

$$E(K_p, s) = E(K_p, D(K_s, h')) = h' \cdots (2 \text{ 式})$$

また、受信者は、受信した平文データ M' を送信者と同じハッシュ関数により圧縮して一定長の出力 h' を算出する演算を行う。そして、この演算で算出された一定長の出力 h' と、上記（2式）により得られた一定長の出力 h' とが一致すれば、受信した平文データ M' が正当であると判断する。

【0006】

平文データ M が送受信間で改ざんされた場合には、上記（2式）により得られた一定長の出力 h' と、受信した平文データ M' を発信者と同じハッシュ関数により圧縮して得られた一定長の出力 h' とが一致しないので改ざんを検出できる。

ここで、平文データ M の改ざんに合わせて電子署名データ s の改ざんも行われてしまうと改ざんを検出することができなくなる。しかし、電子署名データ s を改ざんするには、一定長の出力 h から平文データ M を求める必要があるが、このような計算はハッシュ関数の一方向性により不可能である。

次に、ハッシュ関数について説明する。

【0007】

ハッシュ関数は、電子署名データ s の生成を高速化するため等に用いられる。ハッシュ関数は、任意の長さの平文データ M を処理して、一定の長さの出力（一定長の出力） h を出す機能を持つ。ここで、一定長の出力 h を平文データ M のハッシュ値（またはメッセージダイジェスト、デジタル指紋）という。

ハッシュ関数に要求される性質として、一方向性と衝突耐性がある。一方向性とは、一定長の出力 h を与えた時に、 $h = H(M)$ となる平文データ M の算出が計算量的に困難であることである。衝突耐性とは、平文データ M を与えた時に、 $H(M) = H(M')$ となる平文データ M' ($M \neq M'$) を算出することが計算量的に困難であること、及び $H(M) = H(M')$ かつ $M \neq M'$ となる平文データ M, M' を算出することが計算量的に困難であることである。

ハッシュ関数としては、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128、及びRIPEMD-160等が知られており、これらのアルゴリズムは、一般に公開されている。

【0008】

次に、公開鍵暗号について説明する。

公開鍵暗号は、暗号鍵と復号鍵が異なり、暗号鍵を公開し、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の主な特徴として、以下の3つのことが挙げられる。

(a) 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

(b) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみを秘密に記憶しておけばよい。

(c) 送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【0009】

例えば、平文データ M に対して、公開の暗号鍵 K_p を用いた暗号化操作を $E(K_p, M)$ とし、秘密の復号鍵 K_s を用いた復号化操作を $D(K_s, M)$ とすると、公開鍵暗号アルゴリズムは、次の2つの条件を満たす。

(1) 公開の暗号鍵 K_p が与えられたとき、暗号化操作 $E(K_p, M)$ の計算は容易である。秘密の復号鍵 K_s が与えられたとき、復号化操作 $D(K_s, M)$ の計算は容易である。

(2) もし、秘密の復号鍵 K_s を知らないのなら、公開の暗号鍵 K_p と、暗号化操作 E の計算手順と、 $C = E(K_p, M)$ を知っていても、平文データ M を決定することは計算量の点で困難である。

次に、上記(1)、(2)の条件に加えて、次の(3)の条件が成立することにより、秘密通信を実現できる。

(3) 全ての平文データ M に対し、暗号化操作 $E(K_p, M)$ を定義でき、以下の(4式)が成立する。

$$D(K_s, E(K_p, M)) = M \cdots (4 \text{ 式})$$

つまり、公開の暗号鍵 K_p は公開されているため、誰もが暗号化操作 $E(K_p, M)$ を計算することができるが、復号化操作 $D(K_s, E(K_p, M))$ を計算して平文データ M を得ることができるのは秘密の復号鍵 K_s を持っている本人だけである。

【0010】

一方、上記(1)、(2)の条件に加えて、次の(4)の条件が成立することにより認証通信を実現できる。

(4) すべての平文データ M に対し、復号化操作 $D(K_s, M)$ を定義でき、以下の(5式)が成立する。

$$E(K_p, D(K_s, M)) = M \cdots (5 \text{ 式})$$

つまり、復号化操作 $D(K_s, M)$ を計算できるのは、秘密の復号鍵 K_s を持っている本人のみであり、他の人が偽の秘密の復号鍵 K_s' を用いて復号化操作 $D(K_s', M)$ を計算し、秘密の復号鍵 K_s を持っている本人になりすましたとしても、上記(5式)が成立しない

ので $(E(K_p, D(K_s', M))) \neq M$ 、受信者は、受けとった情報が不正なものであることを確認できる。

【0011】

また、復号化操作 $D(K_s, M)$ が改ざんされても上記(5式)が成立しなくなり $(E(K_p, D(K_s, M))) \neq M$ 、受信者は、受けとった情報が不正なものであることを確認できる。

上記の秘密通信と認証通信とを行うことができる代表例として、RSA暗号やR暗号やW暗号等が知られている。

ここで、現在最も使用されている上記RSA暗号による暗号化と復号は、以下の(6式)で示される。

暗号化: 暗号化鍵 (e, n) 暗号化変換 $C = M^e \pmod{n}$

復号: 復号鍵 (d, n) 復号変換 $M = C^d \pmod{n}$

$n = p \cdot q$

ここで、 p, q は、大きな異なる素数・・・(6式)

このように、米国特許第5499294号明細書には、デジタル画像のハッシュ値に公開鍵暗号を用いた電子署名を作成し、デジタルデータの原本性を保証することが記載されている。

【0012】

【特許文献1】米国特許第5499294号明細書

【発明の開示】

【発明が解決しようとする課題】

【0013】

しかしながら、米国特許第5499294号明細書に記載されている手法では、電子署名をつけたデジタルデータを1ビットでも変更した場合、著者が認めた正当な変更であっても、改ざんとして検出される。さらに、米国特許第5499294号明細書に記載されている手法では、データを変更した後に關しては、その変更したデータが原本でないことだけが分かるだけである。

【0014】

例えば、米国特許第5499294号明細書をデジタルカメラに適用した例を考える。通常、デジタルカメラからの出力であるデジタル画像と電子署名データは、コンピュータ(PC)に取り込まれる。その後、画像が見やすいように輝度を変更したり、フィルタリングをしたり、または画像を小さくするために余計な部分を切り取ったりすることは通常よく行われる。

これらの処理は、画像を見やすく、分かりやすくするための処理であり、デジタル画像の著作者が認めている処理である場合が多い。しかしながら、米国特許第5499294号明細書に記載されている技術では、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

このように従来の技術では、電子署名などによりデータの原本性が保証されているような場合には、上記データを正当なデータとして変更することができないという問題点があった。

【0015】

本発明は上述の問題点に鑑みてなされたものであり、データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにすることを目的とする。

【課題を解決するための手段】

【0016】

本発明の情報処理装置は、所定の作者により作成された原データを処理する情報処理装置であって、前記原データを変更する際に、その変更に関する変更情報を保持する保持手段と、前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする。

また、本発明の他の特徴とするところは、所定の作者により作成された原データを処理する情報処理装置であって、前記原データが原本として保証されたものであることを確認

する原データ確認手段と、前記原データの変更にに関する変更情報が原本として保証されたものであることを確認する変更情報確認手段と、前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、前記変更情報に応じて前記原データを変更する変更手段とを有することにある。

本発明のサーバ装置は、前記何れかに記載の情報処理装置とネットワークで接続されたサーバ装置であって、前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを、前記情報処理装置より受信し、管理することを特徴とする。

本発明の電子データ管理システムは、ネットワークに接続された情報処理装置を複数有する電子データ管理システムであって、前記情報処理装置は、前記ネットワーク上で共有された電子データが原本として保証されたものであることと、前記電子データの変更にに関する第1の変更情報が原本として保証されたものであることを確認する確認手段と、前記電子データと前記第1の変更情報が、前記確認手段により原本として保証されたものであることが確認された場合に、前記電子データを変更する電子データ変更手段と、前記電子データ変更手段により変更された電子データの変更にに関する第2の変更情報と、前記第2の変更情報が原本であることを保証するための変更保証情報とを作成する情報作成手段と、前記情報作成手段により作成された第2の変更情報と、変更保証情報とを前記ネットワークに送信する送信手段とを有し、前記複数の情報処理装置で共同して前記電子データの管理を行うようにしたことを特徴とする。

本発明の情報処理システムは、第1の情報処理装置と、前記第1の情報処理装置とネットワークを介して接続された第2の情報処理装置とを有する情報処理システムであって、前記第1の情報処理装置は、前記第1の情報処理装置から電子データを受信する手段と、前記受信した電子データを変更し、その変更にに関する変更情報と、前記変更情報が原本であることを保証するための第1の変更保証情報とを作成する手段と、前記変更情報と前記第1の変更保証情報を、前記第2の情報処理装置に送信する手段とを有し、前記第2の情報処理装置は、前記第1の情報処理装置により送信された変更情報が原本として保証されたものであることを、前記第1の変更保証情報を用いて確認する手段と、前記変更情報を正当なものとするかを判定する手段と、前記判定手段で正当なものとする判定された場合に、前記変更情報が原本であることを保証するための第2の変更保証情報を作成する手段と、前記第2の変更保証情報を、前記第1の情報処理装置に送信する手段とを有することを特徴とする。

【0017】

本発明の情報処理方法は、所定の作者により作成された原データを処理する情報処理方法であって、前記原データを変更する際に、その変更にに関する変更情報を保持する保持工程と、前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成工程とを行うことを特徴とする。

また、本発明の他の特徴とするところは、所定の作者により作成された原データを処理する情報処理方法であって、前記原データが原本として保証されたものであることを確認する原データ確認工程と、前記原データの変更にに関する変更情報が原本として保証されたものであることを確認する変更情報確認工程と、前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、前記変更情報に応じて前記原データを変更する変更工程とを行うことにある。

【0018】

本発明のコンピュータプログラムは、前記何れかに記載の情報処理方法をコンピュータに実行させることを特徴とする。

本発明のコンピュータ読み取り可能な記憶媒体は、前記記載のコンピュータプログラムを記憶することを特徴とする。

【発明の効果】

【0019】

本発明によれば、所定の作者により作成された原データを変更する際に、その変更にに関する変更情報を保持するとともに、前記変更情報が原本であることを保証するための変更

保証情報を作成するようにしたので、前記変更保証情報に基づいて前記原データの変更が正当なものであるか否かを判断し、正当なものである場合には前記変更情報により前記原データを変更することができるようになる。したがって、前記原データの原本性を保証しながら、前記原データの作者が認める正当な変更を行うことができ、前記原データの原本性と、データの最新性の両方を保証することができる。また、前記変更情報により、前記原データと、変更したデータとの関係を知ることができ、前記原データと、変更したデータとが適切な関係にあることを保証することができる。さらに、前記変更情報は、前記変更したデータそのものに比べてデータ量が少ないので、前記原データを変更するのに要する記憶容量を可及的に小さくすることができる。

【発明を実施するための最良の形態】

【0020】

以下、本発明の実施形態について、図面を参照して詳細に説明する。なお、ここではオリジナルのデジタルデータを原画像と呼ぶが、本実施の形態で適用されるデジタルデータ（原データ）は、デジタル画像だけに限らず、デジタルデータ全てに適用できる。

（第1の実施の形態）

本発明の第1の実施の形態を、図面を参照しながら説明する。

まず、原画像に対する電子署名を生成する。これは、前述した米国特許第5499294号明細書のように、原画像に対するハッシュ値を生成し、そのハッシュ値に対して秘密鍵で電子署名を作成することによって実現できる。この電子署名を第1の署名（図1の署名0）11と表し、図1（a）に示されるように原画像12とともに保存する。

【0021】

次に、保存された原画像12に対して第1の処理を施して、その処理結果を正当な画像として認める場合を考える。ここで、第1の処理とは、画像が見やすいように輝度を変更したり、フィルタリングをしたり、または画像を小さくするために余計な部分を切り取ったりすることなど、原画像に変更を加える処理である。上述した電子署名の原理は、デジタルデータ全てに利用でき、ここでも、上述した電子署名の原理を用いて、履歴情報13に対する電子署名を作成する。つまり、履歴情報13に対するハッシュ値を生成し、そのハッシュ値に対して秘密鍵で電子署名を作成する。

【0022】

ここで、履歴情報13とは、上記第1の処理で行われた原画像12の変更（履歴）に関する情報である。なお、以下の説明では、この履歴情報13に対する電子署名を第2の署名（図1の署名1）14と称する。

例えば、上記第1の処理が、PhotoShop ver.Xというエディタで行った輝度変換である場合、上記第1の処理に対する履歴情報13は、対象画像を特定する情報と、上記エディタを特定する情報と、上記エディタで規定されている輝度変換というフィルタ名と、それに用いたパラメータ情報などから構成される。

また、履歴情報13は、原画像12と変更画像との差分データを含んでいても良い。ここで、対象画像を特定する情報は、原画像12のID番号や、原画像12に対する署名である第1の署名（図1の署名0）11などを用いることができる。そして、このようにして作成された履歴情報13と第2の署名14とを図1（b）に示されるように原画像12と一緒に保存する。

【0023】

上記の処理は、著作者によって行われる処理である。次に、上記第1の処理により輝度変換された画像の入手を他のユーザが希望している場合を考える。著作者は、図1（b）のように、記憶媒体に保存されている原画像12、第1の署名（図1の署名0）11、履歴情報13、及び第2の署名（図1の署名1）14を、通信手段を用いてそのユーザに送信する。

【0024】

以下、これらの情報が送られたユーザが行う検証処理について説明する。

まず、原画像12に対する第1の署名（図1の署名0）11を確認する。原画像12の

著作者の公開鍵を用いて、第1の署名(図1の署名0)11を変換して出力hを得るとともに、原画像12のハッシュ値h'を得て、出力hとハッシュ値h'とが同じであるかを見ることで、第1の署名(図1の署名0)11の確認を行う。

【0025】

次に、履歴情報13に対する第2の署名(図1の署名1)14を確認する。履歴情報13の著作者の公開鍵を用いて、第2の署名(図1の署名1)14を変換して出力hを得るとともに、履歴情報13のハッシュ値h'を得て、出力hとハッシュ値h'とが同じであるかを見ることで、第2の署名(図1の署名1)14の確認を行う。

原画像12と履歴情報13の正当性が第1の署名11と第2の署名14により確認された後、履歴情報13に書かれた情報に基づいて、上記第1の処理と同じ処理を、原画像12に対して行うことにより、ユーザは、輝度変換された画像を得ることができる。

【0026】

図2は、以上のような処理を行う本実施形態の情報処理装置の構成の一例を示したブロック図である。なお、本発明の情報処理装置の実現に当たっては、図2に示される全ての機能を使用することは必須ではない。

図2において、情報処理装置(コンピュータ)301のハードウェアは、一般に普及しているパーソナルコンピュータであり、スキャナ等の画像入力装置317から読み取られた画像を入力し、編集や保管を行うことが可能である。

また、画像入力装置317で得られた画像をプリンタ316から印刷させることができる。なお、ユーザからの各種指示等は、マウス313やキーボード314などからの入力操作により行われる。

【0027】

コンピュータ301の内部では、バス307により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。図2において、MPU302は、コンピュータ301内部の各ブロックの動作を制御し、あるいは内部に記憶されたプログラムを実行することができる。

主記憶装置303は、MPU302において行われる処理のために、一時的にプログラムや処理対象の画像データを格納しておく装置である。ハードディスク(HDD)304は、主記憶装置303等に転送されるプログラムや画像データをあらかじめ格納したり、処理後の画像データを保存したりすることのできる装置である。

【0028】

スキャナインタフェース(I/F)315は、原稿やフィルム等を読み取って、画像データを生成するスキャナ317と接続され、スキャナ317で得られた画像データを入力することのできるインターフェース(I/F)である。

プリンタインタフェース308は、画像データを印刷するプリンタ316と接続され、印刷する画像データをプリンタ316に送信することのできるインターフェース(I/F)である。

【0029】

CDドライブ(CD)309は、外部記憶媒体の一つであるCD(CD-R/CD-RW)に記憶されたデータを読み出したり、あるいは書き込んだりすることができる装置である。

FDDドライブ(FDD)311は、CDドライブ309と同様に、外部記憶装置の一つであるFDD(フレキシブルディスク)からの読み出しや、FDDへの書き込みをすることができる装置である。

DVDドライブ(DVD)310は、FDDドライブ311と同様に、外部記憶装置の一つであるDVDからの読み出しや、DVDへの書き込みをすることができる装置である。

【0030】

なお、CD、FDD、DVD等に画像編集用のプログラム、あるいはプリンタドライバが記憶されている場合には、これらプログラムをハードディスク(HDD)304上にイ

インストールし、必要に応じて主記憶装置 3 0 3 に転送されるようになっている。

インターフェース (I/F) 3 1 2 は、マウス 3 1 3 やキーボード 3 1 4 からの入力指示を受け付けるために、これらと接続されるインターフェース (I/F) である。

また、モニタ 3 0 6 は、透かし情報の抽出処理結果や処理過程を表示することのできる表示装置である。さらに、ビデオコントローラ 3 0 5 は、表示データをモニタ 3 0 6 に送信するための装置である。

なお、本実施の形態では、情報処理装置 3 0 1 に上述した機能を全て搭載するようにしたが、上述した機能を分配して複数の装置からなるシステムとしてもよい。すなわち、複数の機器 (例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等) から構成されるシステムにしても、一つの機器からなる装置 (例えば、複写機、ファクシミリ装置等) にしてもよい。

【0031】

次に、図 3 と図 4 を参照しながら、本実施の形態の情報処理装置 3 0 1 の動作について説明する。図 3 は、電子署名を生成する際の情報処理装置 3 0 1 の処理を説明するフローチャートである。また、図 4 は、電子署名を検証する際の情報処理装置 3 0 1 の処理を説明するフローチャートである。

なお、原画像 1 2 に対する第 1 の署名 (図 1 の署名 0) 1 1 を生成する際の処理は、上述した米国特許第 5 4 9 9 2 9 4 号明細書に記載されている技術と同様にして行えるので説明を省略し、ここでは、原画像 1 2 と第 1 の署名 (図 1 の署名 0) 1 1 が、情報処理装置 3 0 1 内の記憶媒体に保存されているという前提で説明する。

【0032】

まず、図 3 に示す電子署名 (第 2 の署名 (図 1 の署名 1) 1 4) を生成する際の処理を説明する。なお、以下では必要に応じてこの処理を署名生成処理と称する。

記憶媒体に保存された原画像 1 2 を入力する (ステップ S 2 0 1)。これは、ハードディスク (HDD) 3 0 4、CD ドライブ (CD) 3 0 9、DVD ドライブ (DVD) 3 1 0、または FDD ドライブ (FDD) 3 1 1 などに接続された各記憶媒体に格納されている原画像 1 2 を、マウス 3 1 3 やキーボード 3 1 4 からの入力指示により、主記憶装置 3 0 3 にロードすることにより実現される。

【0033】

次に、その原画像 1 2 に対して変更処理を行う (ステップ S 2 0 2)。このときに行った変更処理に関する履歴情報 1 3 を記憶媒体に記憶する (ステップ S 2 0 3)。なお、この変更処理は、複数の処理を組み合わせても良い。

変更処理が正当な処理かを判断する (ステップ S 2 0 4)。

【0034】

ここで、全ユーザのアクセス権限が保存されている不図示のアクセス権限データベースに、そのユーザのアクセス権限が設定されている。そして、上記変更処理の正当性の検証は、図 2 に示すコンピュータへのログイン時に得られる認証情報を基に、上記アクセス権限の範囲内の変更であれば正当と判断する一方、その範囲を超えていれば正当でないと判断することによりなされる。この他、原画像 1 2 の内部やヘッダなどにアクセスに関する許諾範囲を著作者により記述するようにし、それを、変更処理を行うエディタが読み込んで、許諾範囲内の変更であれば正当と判断する一方、許諾範囲を超えていれば正当でないと判断することによっても、上記変更処理の正当性の検証はなされる。

【0035】

また、上記変更処理の正当性の検証を、公開鍵を用いることによっても行うことが可能である。原画像 1 2 に対する第 1 の署名 (署名 0) 1 1 の正当性を見る際には、原画像 1 2 の著作者の公開鍵を用いるが、履歴情報 1 3 に対する第 2 の署名 (署名 1) 1 4 の正当性を見る際にも、先ほど用いた原画像 1 2 の著作者の公開鍵を用いて検証することによって、原画像 1 2 の著作者が変更処理を行ったか否かがわかる。

【0036】

そして、これらの処理は、マウス 3 1 3 やキーボード 3 1 4 からの入力指示に応じて主

記憶装置 303 にロードしたプログラムを、MPU 302 などを用いて実行することにより行われる。このとき、モニタ 306 により実行状況や、その結果をモニタすることも可能である。

このように変更処理の正当性の検証を行い、変更処理した画像が正当であると認められない場合には、処理結果及び処理履歴を廃棄し、前の画像（原画像 12）に戻す。また、変更処理された画像を正当な画像として認める場合、記憶媒体に記憶された履歴情報 13 に対して電子署名（第 2 の署名（図 1 の署名 1）14）を作成する（ステップ S205）。生成した原画像 12、第 1 の署名（図 1 の署名 0）11、履歴情報 13、及び第 2 の署名（図 1 の署名 1）14 を、ハードディスク 304、CD ドライブ 309、DVD ドライブ 310、または FDD ドライブ 311 などに保存する（ステップ S206）。

【0037】

次に、図 4 に示す電子署名を検証する際の処理を説明する。なお、以下では、必要に応じてこの処理を署名検証処理と称する。

なお、電子署名（第 1 の署名 11 及び第 2 の署名 14）の検証処理を行うときには、第 1 の署名（図 1 の署名 0）11、履歴情報 13、及び第 2 の署名（図 1 の署名 1）14 を、情報処理装置 301 が持っていることを前提とする。ただし、以下の処理も、図 2 に示す情報処理装置 301、特に、マウス 313 やキーボード 314 からの入力指示により主記憶装置 303 にロードしたプログラムを、MPU 302 などを用いて実行することにより行われる。

【0038】

まず、原画像 12 に対する第 1 の署名（図 1 の署名 0）11 を確認する（ステップ S211）。これは、原画像 12 に対するハッシュ値を生成し、また、第 1 の署名 11 を原画像 12 の著作者の公開鍵で変換して出力値を得て、ハッシュ値と出力値とが等しければ、原画像 12 が原本であることが保証される。次に、履歴情報 13 に対する第 2 の署名（図 1 の署名 1）14 を確認する（ステップ S212）。これは、履歴情報 13 に対するハッシュ値を生成し、また、第 2 の署名を履歴情報 13 の著作者の公開鍵で変換して出力値を得て、ハッシュ値と出力値が等しければ、履歴情報 13 が原本であることが保証される。

このように、この 2 つのデータ（原画像 12 と履歴情報 13）の正当性が、電子署名（第 1 の署名 11 と第 2 の署名 14）により確認された場合には（ステップ S213）、履歴情報 13 に書かれている処理と同じ処理を原画像 12 に対して行う。これにより、ユーザは、変換処理された画像を得る（ステップ S214）。

【0039】

一方、ステップ S213 において、署名が正しくないと判定された場合には、原画像 12 及び履歴情報 13 のうちの少なくとも何れか一方は正しくないので処理を中止する。また、このように署名が正しくない場合には、情報（原画像 12、履歴情報 13）に改ざんがあることをユーザに通知するようにしてもよい。

以上のように、本実施の形態では、原画像 12 に対する第 1 の署名（図 1 の署名 0）11 を保持するようにしたので、原画像 12 に対する原本性を保証できる。

そして、履歴情報 13 に対する第 2 の署名（図 1 の署名 1）14 を保持するようにしたので、原画像 12 の変更処理に対する正当性を保証できる。したがって、原画像 12 に対して、著作者が認める正当な変更を行うことができ、画像の最新性を保証できる。

【0040】

ところで、上述したように、米国特許第 5499294 号明細書に記載されている技術では、例えば、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

そこで、著作者が自分の署名用の秘密鍵を用いて、変更を認めた変更画像に対して電子署名をつけるという解決策が考えられる。しかしながら、この場合、署名した変更画像は独立した画像となり、原画像 12 と、原画像 12 を変更することにより得られる変更画像との関係が分からなくなるという問題点が残る。さらに、いくつかの変更を著作者が正当と認めた場合、多くの画像と署名のペアを管理する必要があり、メモリの制約もでてく

る可能性がある。

これに対して本実施の形態では、第1の署名（図1の署名0）11及び第2の署名（図1の第2の署名1）14が正しければ、原画像12と変更画像との間の関係（処理履歴）を履歴情報13により知ることができる。

さらに、履歴情報13は、変更画像に比べてデータ量が少ないので、多くの履歴情報13を保存しても、それに対応する変更画像をすべて保存することに比べてメモリ容量が小さくなる。これは、後述する第2の実施の形態に示す複数回の変更処理に対して特に有効である。

また、履歴情報13と署名情報（第1の署名11、第2の署名14）は、画像情報に比べて小さいので、原画像12のヘッダなどに格納することが容易で、多くの履歴情報13があっても1つのファイルとして管理できる。これも後述する第2の実施の形態に示す複数回の変更処理に対して特に有効である。

【0041】

（第2の実施の形態）

次に、本発明の第2の実施の形態を説明する。なお、本実施の形態の説明において、第1の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

第1の実施の形態では、1回の処理に対する例を示したが、本実施の形態では、第1の処理の後に、第2の処理、第3の処理・・・と続けて、複数回の処理を正当な処理として認められるようにしている。すなわち、本実施の形態では、以下に示すようにして、原画像12の原本性を保証しながら、複数回の変更処理による画像の最新性を保証できるようにしている。ここで、第2の処理、第3の処理・・・は、第1の処理と同様に、画像に変更を加える処理である。

【0042】

ここで、第1の実施の形態の情報処理装置301で生成した履歴情報13を第1の履歴（図5の履歴1）と表す。第1の実施の形態では、図3のフローチャートに従って行われる処理の前提として、原画像12と第1の署名（図5の署名0）11は保存されているとしたが、本実施の形態では、2回目の変更に対しては第1の履歴（図5の履歴1）13と、第1の履歴（図5の履歴1）13に対する第2の署名（図5の署名1）14も保存されているとして、図3のフローチャートに従った処理を行う。

【0043】

その結果、2回目の変更に対する履歴情報として第2の履歴（図5の履歴2）15と、この第2の履歴15に対する電子署名である第3の署名（図5の署名2）16とが生成される。その結果、原画像12、第1の署名（図5の署名0）11、第1の履歴（図5の履歴1）13、及び第2の署名（図5の署名1）14に加えて、第3の履歴（図5の履歴2）15と第2の署名（図5の署名2）16とが保存される。

以下同様にして変更処理を繰り返せば、N（Nは自然数）回の変更処理に対して、原画像12と、第1～第Nの履歴（図5の履歴1～履歴N）と、第1～第（N+1）の署名（図5の署名0～署名N）とが署名生成処理によって生成され、保存されることになる（図5（a）を参照）。

【0044】

一方、この署名生成処理に対する署名検証処理では、図4のフローチャートにおけるステップS211の処理、すなわち原画像12に対する署名確認の処理を行った後に、ステップS212において、第2の署名（署名1）13の検証だけでなく、第3～第N+1の署名（図5の署名2～署名N）についても検証を行う。そして、ステップS213において、これら第2～第（N+1）の署名（図5の署名1～署名N）が正しいと判断された場合には、ステップS214において、原画像12に対し、第1～第Nの履歴（図5の履歴1～履歴N）の処理を実行し、原画像12を変更する。

【0045】

なお、この場合において、第2～第M（Mは、（N+1）より小さい自然数）の署名までは正しく、それ以降の署名が正しくない場合には、全ての処理を中止しなくても第2～

第Mの署名に対する第1～第M-1の履歴の処理を行い、第M+1～第N+1の署名に対する第M～第Nの履歴の処理を中止することもできる。また、第2～第(N+1)の署名(図5の署名1～署名N)全てを正しいか判定してから、第1～第Nの履歴(図5の履歴1～履歴N)の処理を実行するのではなく、第2の署名が正しいければ、第1の履歴の処理を実行し、その後、第3の処理が正しいければ、第2の履歴を処理を実行するというように、検証と変更処理を交互に繰り返しても構わない。

【0046】

以上のように本実施の形態では、1～N回目の変更に対する履歴情報である第1～第Nの履歴と、この第1～第Nの履歴に対する電子署名である第2～第(N+1)の署名とを生成するようにし、第1～第Nの履歴が正しいかどうかを、第2～第(N+1)の署名を用いて判断し、正しい場合には第1～第Nの履歴に従って原画像12を変更するようにしたので、1回の変更だけでなく、著作者が正当と認めれば複数回の変更処理を追加しても画像の最新性を常に保証できる。

【0047】

なお、著作者が、第1の処理を含まない新たな第2の処理も正当と認める場合には、第1の処理の代わりに第2の処理の履歴情報に対して図3と図4に示したフローチャートに従った処理を行えば、第2の処理に対する変更の正当性と原本性が第1の実施の形態と同様にして保証できることは明らかである。この場合、第1の処理と第2の処理に関する関係は、図5(b)のようになる。このとき、図6に示すようなリスト60に、履歴情報と電子署名とを処理ごとにまとめて別管理したり、履歴情報のなかにその処理の目的・効果などのアブストラク的な情報を入れておいたりすることもできる。この履歴情報と電子署名に関する管理は管理データベースを設け、行った変更毎にそのデータベースに登録することによって実現できる。ユーザは必要なときにそのデータベースを参照する。

【0048】

(第3の実施の形態)

本発明の第3の実施の形態を説明する。なお、本実施の形態の説明において、第1及び第2の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

第1及び第2の実施の形態では、処理の変更はすべて著作者が行う例を示したが、本実施の形態では、多くのユーザが1つのデジタルデータを変更することができるようにする。ここでは、デジタルデータとして電子文書を想定する。そして、図7に示すように、複数のユーザ603～605がサーバ601上で電子文書602を共有しており、ネットワーク600を介して各ユーザ603～605が電子文書602を作成及び変更する場合を想定する。

【0049】

なお、ユーザ603～605とは、ユーザが所有する端末のことであり、この端末のハードウェアは、例えば図2に示した情報処理装置301により構成されるものである。以下、サーバ601及びユーザ603～605における処理の内容について説明する。

まず、ユーザ603が最初のたたき台となる電子文書602を作成し、作成した電子文書602を第1の文書として、第1の文書に対する署名をつけてサーバ601に保存する。なお、以下の説明では、第1の文書に対する署名を第1の署名と称する。また、この第1の署名は、第1及び第2の実施の形態で説明した第1の署名(署名0)11と同じ方法で作成される。

【0050】

次に、サーバ601に保存された電子文書602をユーザ604が修正したい場合、ユーザ604は、まず、第1の文書と第1の文書に対する第1の署名を確認する。すなわち、第1及び第2の実施の形態と同様に、第1の文書に対するハッシュ値を生成し、また、第1の署名を第1の文書の著作者の公開鍵で変換して出力値を得て、ハッシュ値と出力値とが等しければ、第1の文書が原本であることが保証される。第1の署名が正当であれば、第1の文書に対して修正を施して第2の文書を作成し、第1の文書の修正に関する第1の履歴情報と、この履歴情報に対する第2の署名を付加して保存する。第1の履歴情報と

第 2 の署名は、それぞれ第 1 及び第 2 の実施の形態で説明した第 1 の履歴情報（履歴 1）1 3 と第 2 の署名（署名 1）1 4 と同じ方法で作成される。

【0 0 5 1】

ここで、全ユーザのアクセス権限が保存されている不図示のアクセス権限データベースに、そのユーザのアクセス権限が設定されている。そして、上記変更処理の正当性の検証は、各ユーザが図 2 に示すコンピュータへログインする時に得られる認証情報を基に、そのアクセス権限の範囲内の変更であれば正当と判断する一方、その範囲を超えた変更であれば正当でないと判断することによって行うことができる。この他、最初の著作者であるユーザ 6 0 3、もしくは図 7 のシステムによって、電子文書の内部やヘッダなどにアクセスに関する許諾範囲を設定するようにし、それを、変更処理を行うエディタが読み込んで、許諾範囲内の変更であれば正当と判断する一方、許諾範囲を超えていれば正当でないと判断することによって、上記変更処理の正当性の検証を行ってもよい。

【0 0 5 2】

また、上記変更処理の正当性の検証を、公開鍵を用いることによって行うことが可能である。この場合は、ユーザごとの秘密鍵も用いて署名を生成するのではなく、変更が認められたグループの秘密鍵を用いて署名を生成し、そのグループの公開鍵を用いて、検証を行う。第 1 の文書に対する第 1 の署名の正当性を見る際には、このグループの公開鍵を用い、また、第 2 の履歴情報に対する第 2 の署名の正当性を見る際にも、先ほど用いたグループの公開鍵を用いて検証することによって、グループ内の誰かが変更処理を行ったことがわかる。

このように、他のユーザまたは同じユーザが文書の修正を繰り返したい場合、修正に関する履歴情報と、この履歴情報に対する署名を付加していくことにより、複数のユーザによる電子文書の管理を実現することができる。

【0 0 5 3】

ただし、あるユーザが、それまでの署名を確認したときに、署名が正当でなければその旨を他のユーザに通知する。また、あるユーザが、第 1 ～第 M（M は自然数）の履歴情報までの修正は良いと思うが、それ以降の修正は良くないと思う場合には、良いと思う履歴情報までの修正を行った第 M の文書を作成し、そのあと第（M + 1）の履歴情報とは異なる修正を行う。その後、第 M の文書を対象文書として特定する情報（文書番号やハッシュ値など）を履歴情報に入れて、その署名を作成することもできる。この場合、第 2 の実施の形態で説明した図 5（b）のように、作成した署名がそれまでの署名と並列の関係になるので、文書管理システムの中に図 6 のような署名の関係を示すリスト 6 0 を作成し、分かりやすくすることも可能である。

【0 0 5 4】

（第 4 の実施の形態）

本発明の第 4 の実施の形態を説明する。なお、本実施の形態の説明において、第 1 ～第 3 の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。本実施の形態では、医療画像に対する医療画像管理システムを例にとり説明する。

システムとしては、図 7 と同様に、複数のユーザ（医者）6 0 3 ～6 0 5 がデジタルレントゲン画像などの電子化された医療画像 6 0 2 をネットワーク 6 0 0 で接続されたサーバ 6 0 1 上に共有している場合を想定する。

この場合、医療画像 6 0 2 に対する原本性を保証するための情報である第 1 の署名は、デジタルレントゲン機器に保存されているか、またはデジタルレントゲン機器における医療画像 6 0 2 の出力時点で生成され、サーバ 6 0 1 に保存されているとする。

【0 0 5 5】

まず、医者 6 0 3 が医療画像 6 0 2 を見る場合、画像内容に関する編集は行わないが輝度変換などの視覚的効果に関する変更を行う。このとき、医者 6 0 3 は、毎回その輝度変更を行わないようにするために、原画像である医療画像 6 0 2 と変更画像との差分をとり、対象画像を特定する情報や上述したその変更に関するアブストラク的な情報を、医療画像 6 0 2 に付加して第 1 の履歴情報として保存する。

そして、この第1の履歴情報のハッシュ値に自分の署名を生成し、第2の署名としてサーバ601に保存するか、または自分（医者603）が所有する端末に保存する。なお、これら第1の履歴情報と第2の署名は、それぞれ第1～第3の実施の形態で説明した第1の履歴情報（履歴1）13と第2の署名（署名1）14と同じ方法で作成される。

【0056】

次に、医者604が医療画像602を見る場合、その原本性を第1の署名により確認し、他の医者603の処理を確認するために第1の履歴情報の正当性を第2の署名により確認し、それを利用またはさらに処理を追加する。

ここで、処理を追加する場合は、第1の履歴情報に従った変更が施された医療画像を変更対象とする場合には、変更対象とする画像に対する情報として第2の署名を第2の履歴情報に含め、さらに、変更対象とする画像と、自分が作成した変更画像との差分画像などを加えて、第3の署名を生成する。また、原画像（医療画像602）を変更対象とする場合、第1の署名を第2の履歴情報に含め、さらに、原画像（医療画像602）と、自分が作成した変更画像との差分画像などを加えて、第3の署名を生成する。

【0057】

以下、同様の処理を行うことにより、本実施の形態の医療画像管理システムにおいて、原画像の原本性と変更処理の正当性、及び画像の最新性を同時に実現できる。なお、上記において、第2の履歴情報と第3の署名は、それぞれ第2～第3の実施の形態で説明した第2の履歴情報（履歴2）15と第3の署名（署名2）16と同じ方法で作成される。

【0058】

（第5の実施の形態）

本発明の第5の実施の形態を説明する。なお、本実施の形態の説明において、上述した第1～第4の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。本実施の形態では、著作物管理システムを用いたビジネスモデルに関する説明を行う。ここでは、ネットワークに複数のユーザと原画像に対し1次著作権を保有する著作権者がある場合を考える。よって、著作権者は、図1（a）のように、原画像12とそれに対する第1の署名（署名0）11を有しているとする。

【0059】

図8のフローチャートを参照しながら、本実施の形態のシステムにおける処理を説明する。

まず、著作権者は、課金などにより正当と認められたユーザに対して、原画像12を配布する（ステップS701）。ただし、この原画像12には、電子透かしなどの著作権保護のための仕組みが入っていても良い。また、この原画像12には、上述した原本性を示す第1の署名（署名0）11も添付されている。配布された原画像12については、ユーザの利用範囲内で変更することが認められているが、原画像12を含むその変更画像の配布は認められていないとする。

【0060】

ユーザは、各々、原画像12の署名を確認した後、著作権者から配布された原画像12に対して、いくつかの変更を試みる（ステップS702）。ユーザが面白いと思った変更画像を正当な2次著作物としたい場合、ユーザは、著作権者に、原画像12と第1の署名（署名0）11に加えて自ら行った変更に関する履歴情報である第1の履歴情報13とその電子署名である第2の署名（署名1）14を著作権者に送る（ステップS703）。ただし、第2の署名（署名1）14は、ユーザの秘密鍵で署名されており、それを確認する公開鍵も一緒に送付することができる。

【0061】

著作権者は、第1の署名（署名0）11と、第2の署名（署名1）14を確認し、原画像12に対して第1の履歴情報13に応じた処理を施す（ステップS704）。著作権者がその処理結果を判定して（ステップS705）、2次著作物として許諾する場合には、第1の履歴情報13に対して著作権者の秘密鍵による電子署名を生成し、原画像12と第1の署名（署名0）11と、第1の履歴情報13と、第2の署名（署名1）14と、第3の署名

(署名2) 16とを一緒に保存する(ステップS706)。一方、許諾しない場合は第3の署名(署名2) 16を生成せずに、その旨をユーザに通知する。

【0062】

このように、本実施の形態では、原画像12の著作者が変更処理を認める場合は、変更処理に対する署名を著作者の秘密鍵で生成するので、著作者は、原画像12である1次著作物から効率的に2次著作物を生成する仕組みを実現することができ、各ユーザは、自分が生成した2次著作物を正当に認められる仕組みを実現することができる。また、このとき、著作者は複数の2次著作物を許可し、その後、著作権料を得ることも可能である。各ユーザは1次著作物を基に容易に2次著作物を生成でき、それによる2次著作権料も得ることができる。さらに、3次著作物以降に対しても全く同様にして適用できる。

【0063】

(その他の実施の形態)

本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体(または記憶媒体)を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ(またはCPUやMPU)が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本発明を構成することになる。

【0064】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0065】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【図面の簡単な説明】

【0066】

【図1】本発明の第1の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図2】本発明の第1の実施の形態を示し、情報処理装置の構成の一例を示したブロック図である。

【図3】本発明の第1の実施の形態を示し、電子署名を生成する際の処理を説明するフローチャートである。

【図4】本発明の第1の実施の形態を示し、電子署名を検証する際の処理を説明するフローチャートである。

【図5】本発明の第2の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図6】本発明の第2の実施の形態を示し、履歴情報と電子署名とを処理ごとにまとめたリストの一例を示した図である。

【図7】本発明の第3の実施の形態を示し、電子データ管理システムの構成の一例を示したブロック図である。

【図8】本発明の第5の実施の形態を示し、著作物管理システムで行われる処理を説

明するフローチャートである。

【符号の説明】

【 0 0 6 7 】

1 1、1 4、1 6 電子署名

1 2 原画像

1 3、1 5 履歴情報

3 0 1 情報処理装置

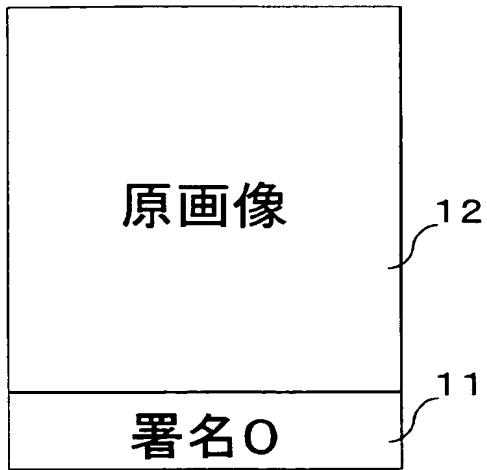
6 0 1 サーバ

6 0 2 電子文書

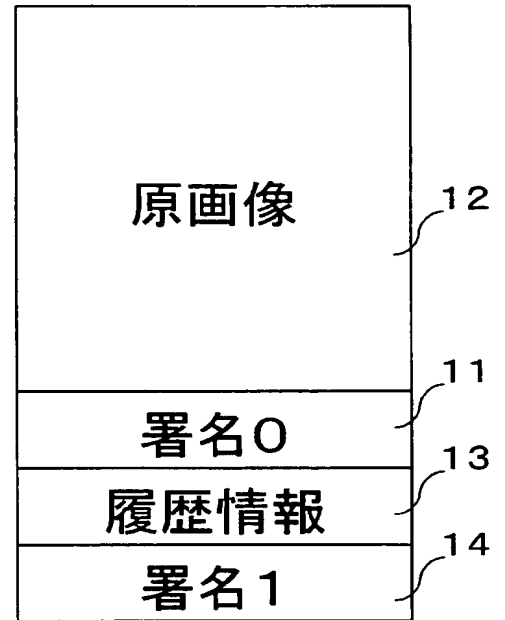
6 0 3 ~ 6 0 5 ユーザ

【書類名】 図面

【図 1】

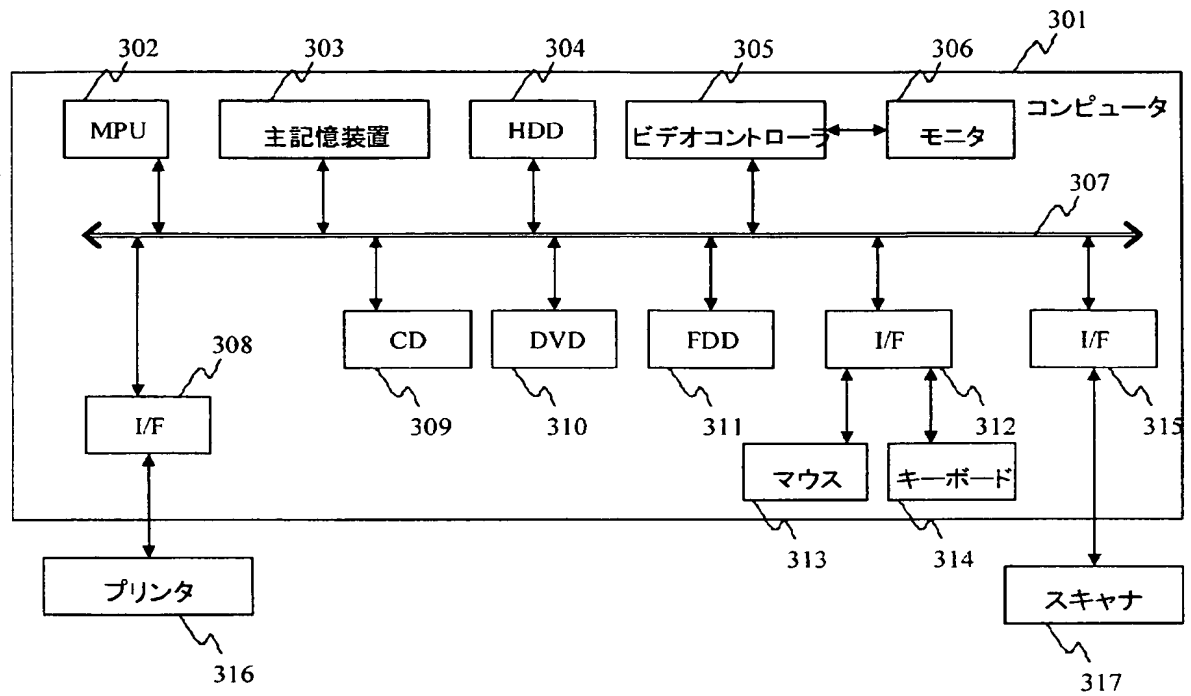


(a)

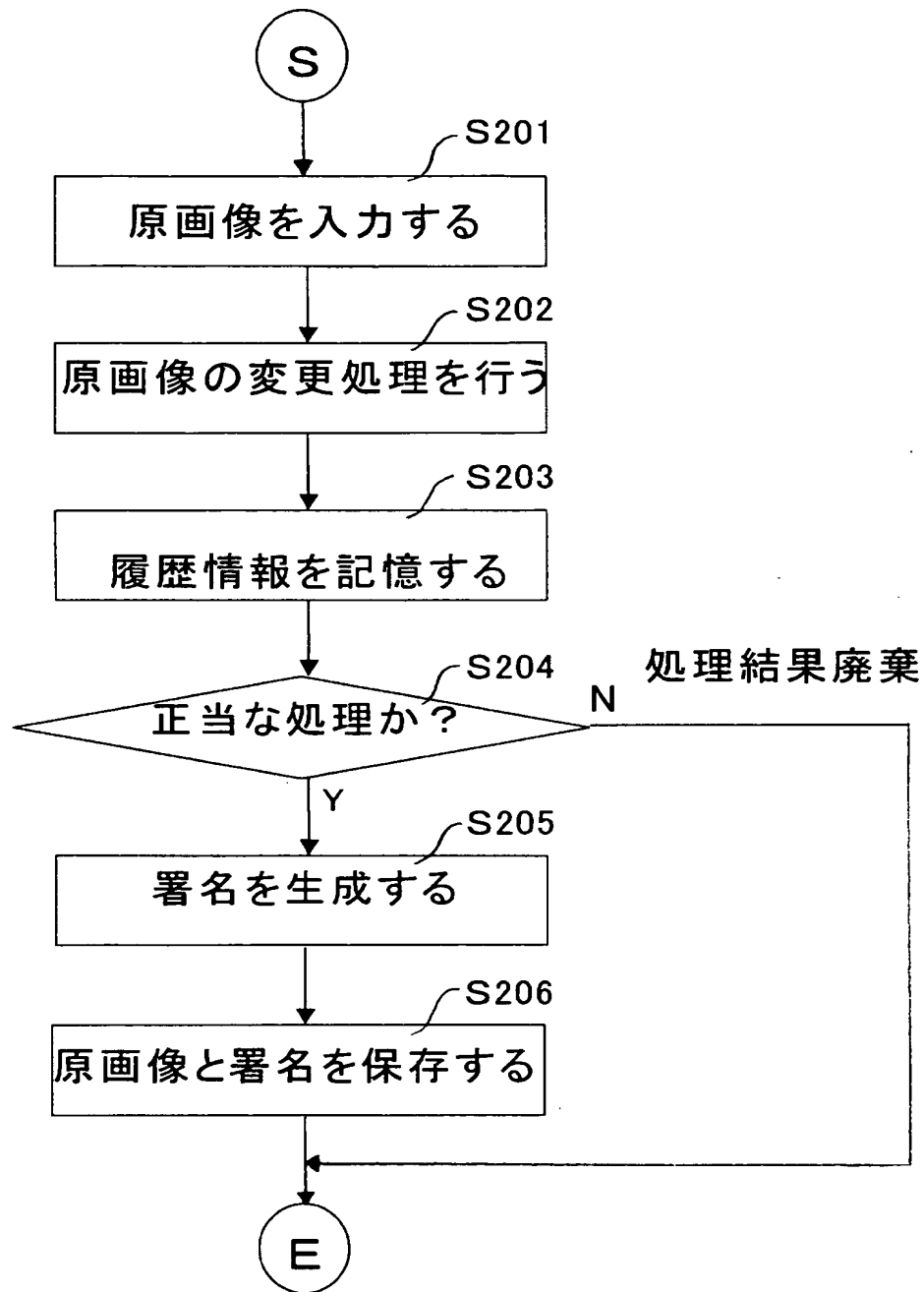


(b)

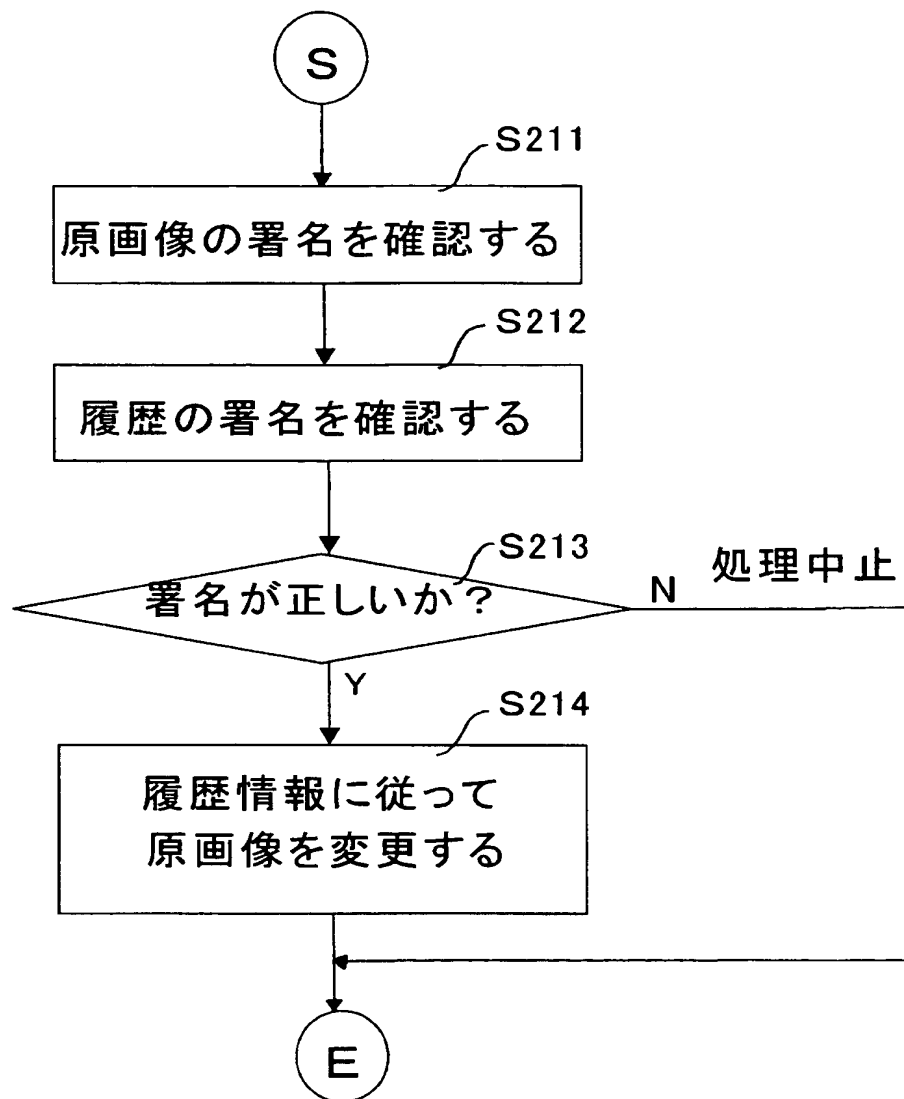
【図 2】



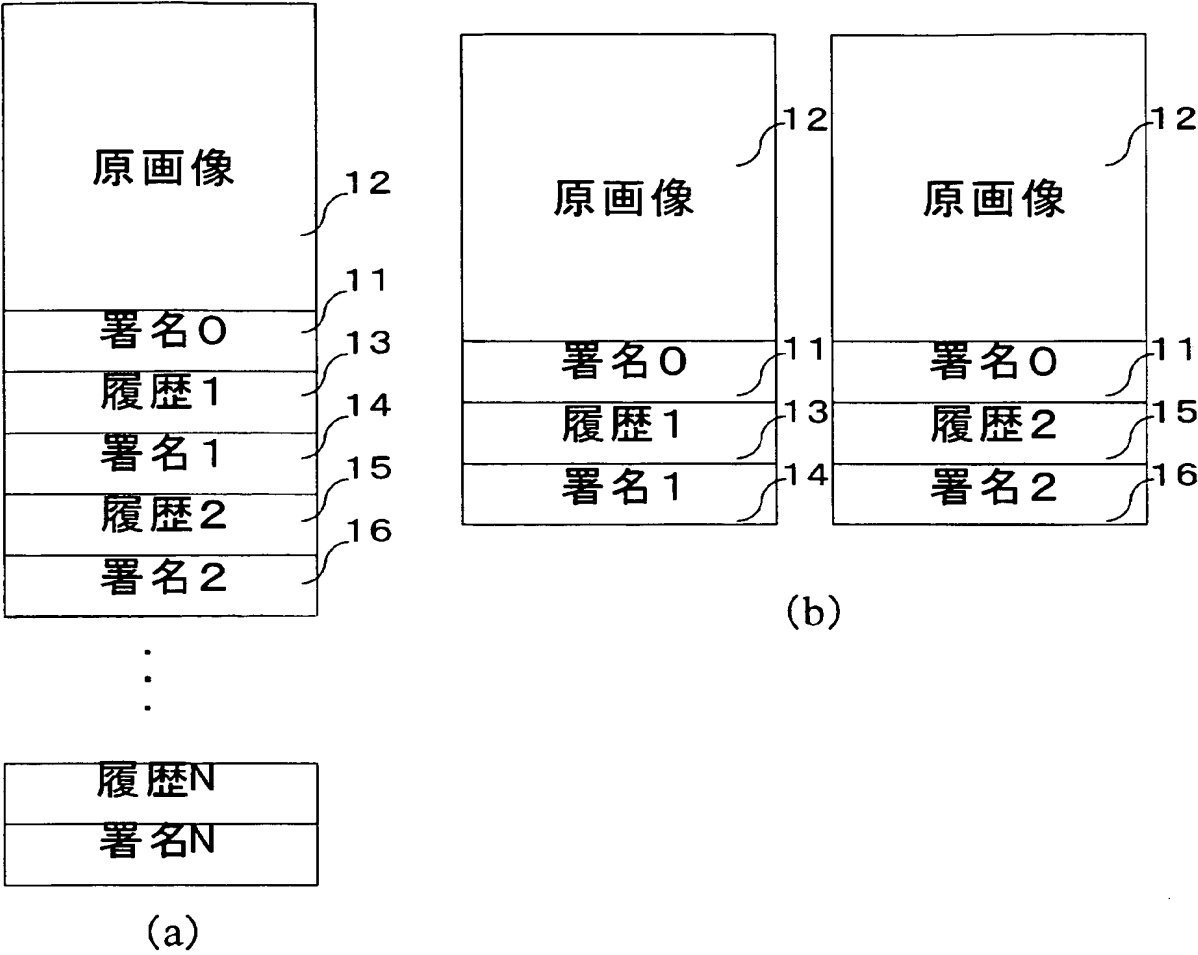
【図 3】



【図 4】



【図 5】

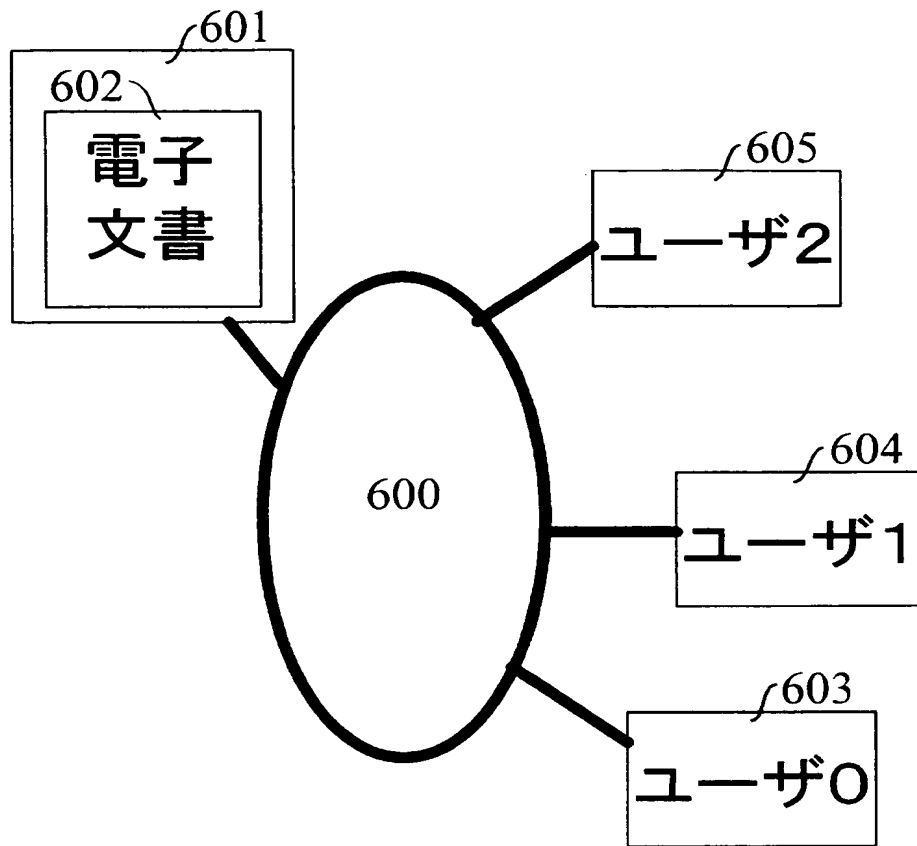


【図 6】

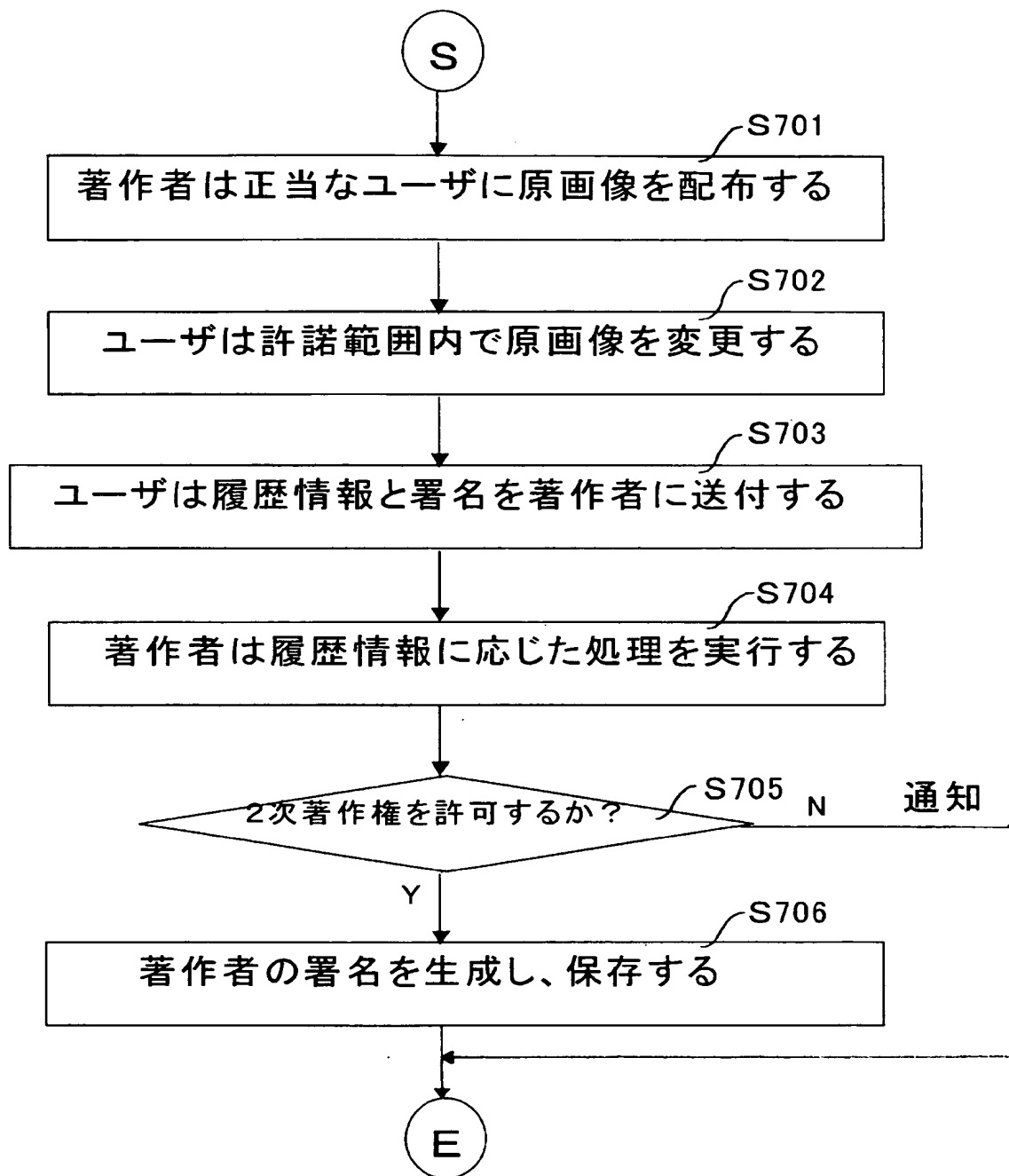
60

履歴情報	電子署名	用途
履歴 1	署名 1	輝度変換
履歴 2	署名 2	切り取り
・ ・ ・	・ ・ ・	・ ・ ・

【図 7】



【図 8】



【書類名】 要約書**【要約】**

【課題】 データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにする技術を提供することを目的とする。

【解決手段】 所定の作者により作成された原データ（原画像 1 2）を処理する情報処理装置であって、上記原データを変更する際に、その変更に関する変更情報（履歴情報 1 3）を記憶媒体に記憶する変更情報記憶部と、上記変更情報が原本であることを保証するための変更保証情報（第 2 の署名（署名 1） 1 4）を作成する変更保証情報作成部とを有することを特徴とする。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2003-346140
受付番号	50301652506
書類名	特許願
担当官	第三担当上席 0092
作成日	平成15年10月 8日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子3丁目30番2号
【氏名又は名称】	キャノン株式会社

【代理人】

【識別番号】	100090273
【住所又は居所】	東京都豊島区東池袋1丁目17番8号 池袋TG ホームストビル5階 國分特許事務所
【氏名又は名称】	國分 孝悦

特願 2 0 0 3 - 3 4 6 1 4 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 0 0 7]

1 . 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キヤノン株式会社